



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,658	07/21/2003	Wolfgang S. Hammersmith	44461660-8127	7014

26263 7590 08/08/2007
SONNENSCHN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER

PERUNGAVOOR, VENKATANARAY

ART UNIT	PAPER NUMBER
----------	--------------

2132

MAIL DATE	DELIVERY MODE
-----------	---------------

08/08/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/624,658

Applicant(s)

HAMMERSMITH ET AL.

Examiner

Venkat Perungavoor

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 July 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 July 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>12/03 & 1/04</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-5, 18-19 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6886098 to Benaloh.
3. Regarding Claim 1,18 Benaloh discloses the combining the cryptographic key with another key to form a key set see Fig. 3 item 306 & Col 6 Ln 13-20; unfolding the previous transport key to form an unfolded key see Abstract & Col 12 Ln 5-17; encrypting the key set using a public key to form a encrypted key set see Col 12 Ln 18-25; distributing the key set across a medium see Fig.11 & Col 12 Ln 25-33; decrypting the key set to reconstitute the cryptographic key and another key see Col 12 Ln 50-58.
4. Regarding Claim 2, Benaloh discloses the combining, unfolding, encrypting and distributing performed by first party(provider) see Col 14 Ln 41-44; decrypting step performed by the player for entering secure communications see Col 16 Ln 11-22.

Art Unit: 2132

5. Regarding Claim 3, Benaloh discloses the recovering of key from a collection of keys see Col 16 Ln 11-22 & Col 18 Ln 11-20.
6. Regarding Claim 4, Benaloh discloses the compression of keys and decompression keys see Col 18 Ln 41-52.
7. Regarding Claim 5, Benaloh discloses the reverse of a key folding process using bit swapping see Col 19 Ln 25-37.
8. Regarding Claim 19, Benaloh discloses the generating cryptographic key 308, transport key see 310, unfolding the key to form a new key see Fig. 3 item 318, encrypting the key set see Fig. 6 item 400, distributing the key set see Fig.11 & Col 12 Ln 25-33

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
 - (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
10. Claim 6-7, 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6886098 to Benaloh in view of US Patent 7194090 to Muratani et al.(hereinafter Muratani).
11. Regarding Claim 6-7, Benaloh discloses the splitting each byte of key into new bytes see Fig. 17 item 1702 & 1704. But does not disclose the moving the MSB into the LSB of new byte

of unfolded key and padding the MSB of new byte with identical bits. However, Muratani discloses the moving the MSB into LSB of new byte see Fig. 34A and padding the MSB of new byte with identical bits see Col 14 Ln 30-38. It would be obvious to one having ordinary skill in the art at the time of the invention to include the moving the MSB into LSB of new byte and padding the MSB of new byte with identical bits in the invention of Benaloh in order to randomize the key as taught in Abstract.

12. Regarding Claim 12-13, Benaloh discloses the combining, unfolding, encrypting, distributing and decrypting see Col 14 Ln 41-44 & Col 16 Ln 11-22. But does not explicitly disclose the iterations. However, Muratani discloses the iterations see Fig. 23. It would be obvious to one having ordinary skill in the art at the time of the invention to include iterations in the invention of Benaloh in order to increase the randomness as taught in Muratani see Fig. 49 item 1001n.

13. Claim 8-11, 14-17, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6886098 to Benaloh in view of US Patent 2003/0149876 to McGough.

14. Regarding Claim 8-10, Benaloh does not disclose the ASCII character set and OTP. However, McGough discloses the ASCII character set see Par. 0010 and OTP see Fig. 3 item 27. It would be obvious to one having ordinary skill in the art at the time of the invention to include ASCII character set in the invention of Benaloh in order to easily attain a sequence of characters as taught in McGough see Par. 0015.

15. Regarding Claim 11, Benaloh does not disclose the encryption/decryption using the same key. However, McGough discloses the same key for encryption/decryption see Par. 0093. It would be obvious to one having ordinary skill in the art at the time of the invention to include the encryption/decryption using the same key in the invention of Benaloh in order to have symmetric encryption and transfer of keys as taught in McGough see Fig. 1 item "Key Exchange".

16. Regarding Claim 14-17, 20, Benaloh does not disclose the XORing function, conversion key and true random number generator and ASCII. However, McGough discloses the XORing function see Par. 0127, conversion key see Fig. 3 item 11, true random number generator see Fig. 1 item 103 and ASCII character set see Par. 0010.

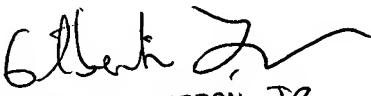
Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8:30-5:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

18. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VP/
Venkat Perungavoor
Examiner
Art Unit 2132
August 3, 2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100